11 MAY 2023 ISSUE 5

WEEKLY
CYBER SECURITY BRIEFING

Armoryze
Be More Secure

US GOVERNMENT TAKES DOWN TRY2CHECK, A MAJOR DARK WEB CREDIT CARD VERIFICATION PLATFORM

We are pleased to share with you a recent victory against cybercrime, as the US government has partnered with law enforcement agencies in Germany and Austria to dismantle Try2Check, a platform used by criminals to verify stolen credit card numbers before selling them online. The operator of Try2Check, Denis Gennadievich Kulkov, has been indicted on charges of access device fraud, computer intrusion, and money laundering.

This platform processed tens of millions of stolen credit card numbers each year, making it a key enabler of the trade in stolen credit card information. However, the takedown of this criminal network demonstrates that the US government and its partners will disrupt cybercrime operations, regardless of their location.

This case highlights the need for businesses to take measures to protect against cybercrime, particularly for companies handling sensitive data. These measures include implementing security protocols, providing regular employee training on cybersecurity awareness, and performing regular security audits. Compliance with the Payment Card Industry Data Security Standard (PCI DSS) is also essential to prevent cybercriminals from exploiting vulnerabilities in payment processing systems.

At Armoryze, we understand the importance of maintaining full PCI DSS compliance to protect your business from cyber threats. Our team of experts is ready to assist you in achieving and maintaining this vital certification. Schedule a **FREE consultation** with our PCI expert today to take the first step in protecting your customers' data from cyber threats.

11 MAY 2023 ISSUE 5

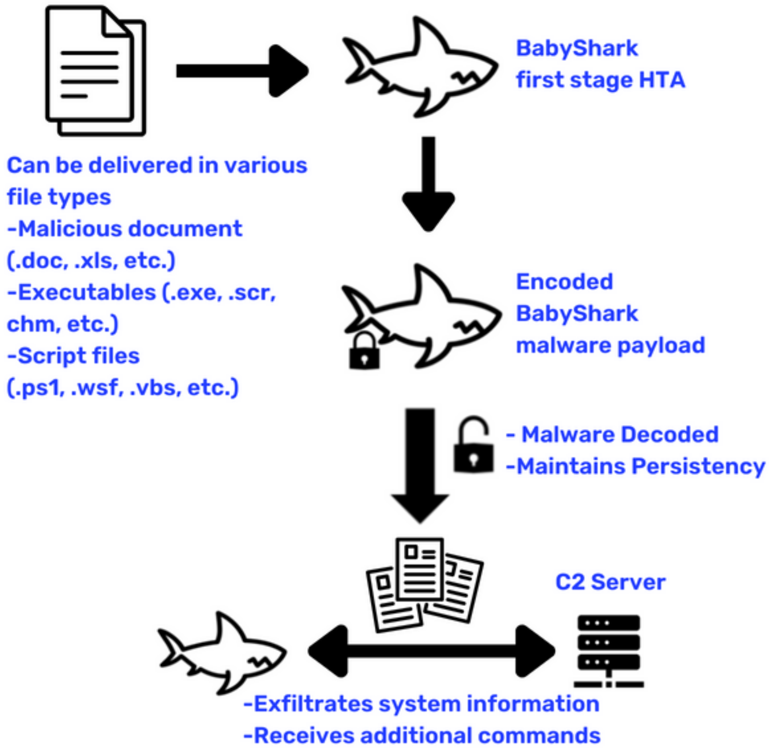
WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

RECONSHARK: THE LATEST THREAT FROM NORTH KOREAN STATE-SPONSORED GROUP KIMSUKY

Kimsuky, a state-sponsored threat group from North Korea, is using a new reconnaissance tool called ReconShark to gain a foothold on compromised hosts and stealthily gather intelligence for extended periods of time. The malware is actively delivered to targeted individuals via spear-phishing emails, OneDrive links that lead to document downloads, and the execution of malicious macros. Once executed, ReconShark exfiltrates system information to a command-and-control server, maintains persistence on the system, and waits for further instruction from the operator.

The spear-phishing emails are designed with a level of quality that is tailored to specific individuals, increasing the likelihood of opening by the target. The messages contain links to booby-trapped Microsoft Word documents hosted on OneDrive to deploy ReconShark, which functions primarily as a reconnaissance tool to execute instructions sent from an actor-controlled server. It is also an evolution of the threat actor's BabyShark malware toolset.


BabyShark
first stage HTA
Can be delivered in various file types
-Malicious document (.doc, .xls, etc.)
-Executables (.exe, .scr, chm, etc.)
-Script files (.ps1, .wsf, .vbs, etc.)
Encoded BabyShark malware payload
- Malware Decoded
-Maintains Persistency
C2 Server
-Exfiltrates system information
-Receives additional commands

ReconShark exfiltrates details about running processes, deployed detection mechanisms, and hardware information, suggesting that data gathered from the tool is used to carry out "precision attacks" involving malware tailored to the targeted environment in a manner that sidesteps detection. The malware is also capable of deploying additional payloads from the server based on what detection mechanism processes run on infected machines. Furthermore, ReconShark does not save the harvested information on the file system, instead opting to store the data in string variables and uploading it to the C2 server by issuing HTTP POST requests.

The ongoing attacks from Kimsuky and their use of the new reconnaissance tool, ReconShark, highlight the evolving nature of the North Korean threat landscape. Organizations should educate their employees on the risks of spear-phishing emails and implement security measures such as anti-phishing filters and endpoint protection solutions to detect and prevent attacks. Additionally, regular security training and testing should be conducted to ensure that employees are aware of the latest threats and how to respond appropriately.

Finally, organizations should keep their **security monitoring solutions** up to date to proactive detect, respond and contain any malware intrusions. Armoryze offers a free trial to help organizations identify, alert and respond to cyber threats & attacks using the cloud native SIEM solution.

CRITICAL SECURITY ALERT: OVER 1 MILLION WEBSITES AT RISK OF XSS EXPLOIT DUE TO A WORDPRESS PLUGIN VULNERABILITY

Two widely used WordPress plugins, "Advanced Custom Fields" and "Advanced Custom Fields Pro," have been found to be vulnerable to cross-site scripting (XSS) attacks. The vulnerability was classified as a high-severity reflected XSS vulnerability (CVE-2023-30777) and was discovered by security researchers at Patchstack on May 2, 2023. The plugins have over 2 million active installations worldwide, making them among the most widely used custom field builders for WordPress websites.

Even default installations of the plugins can trigger the vulnerability, and logged-in users with access to the plugin can trigger the XSS. However, unauthenticated attackers would still need to social engineer someone with access to the plugin to visit a malicious URL to exploit the flaw. The vulnerability was fixed in version 6.1.6, which was released on May 4, 2023. The flaw was due to the 'admin_body_class' function handler, which did not properly sanitize the output value of a hook that controls and filters the CSS classes for the main body tag in the admin area of WordPress sites. Attackers could exploit this vulnerability by leveraging an unsafe direct code concatenation on the plugin's code to add harmful code (DOM XSS payloads) in its components that will pass to the final product, a class string. The cleaning function used by the plugin, 'sanitize_text_field,' will not stop the attack because it won't catch the malicious code injection. The developer fixed the flaw by implementing a new function named 'esc_attr' that properly sanitizes the output value of the admin_body_class hook, preventing the XSS. All users of Advanced Custom Fields and Advanced Custom Fields Pro are advised to upgrade to version 6.1.6 or later immediately.

CACTUS RANSOMWARE: A NEW THREAT EXPLOITING VPN VULNERABILITIES

CACTUS RANSOMWARE
YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34

Ransomware attacks have become increasingly prevalent and sophisticated, and the latest discovery of the "CACTUS" variant is no exception. This insidious malware leverages known vulnerabilities in VPN appliances to gain initial access to targeted networks, allowing the perpetrators to employ custom scripts to deploy and detonate the ransomware encryptor via scheduled tasks. What's even more concerning is that the ransomware has been observed targeting large commercial entities, employing double extortion tactics to steal sensitive data before encrypting it.

CACTUS uses various tactics to evade detection and monitoring tools, making it extremely difficult to detect and stop. It employs Cobalt Strike and Chisel for command-and-control, as well as remote monitoring and management software to push files to infected hosts. It disables and uninstalls security solutions, extracts credentials from web browsers and the Local Security Authority Subsystem Service (LSASS), conducts lateral movement and data exfiltration, and even encrypts itself.

To protect themselves from these threats, companies should keep their systems updated and implement the Principle of Least Privilege (PoLP). Additionally, the Zero Trust security model can greatly reduce the risk of a ransomware attack by assuming that all users and devices are untrusted until they can be verified and authenticated, restricting access to only necessary resources.

The rise of CACTUS and other ransomware families like Rapture, Gazprom, BlackBit, UNIZA, Akira, and Kadavro Vector underscores the need for companies to remain vigilant and take proactive measures to protect themselves from the scourge of ransomware.

WEEKLY
CYBER SECURITY BRIEFING

Armoryze
Be More Secure

US STRIKES BACK: 'SNAKE' CYBERESPIONAGE MALWARE FROM RUSSIA NEUTRALIZED

The US government has successfully neutralized Snake, the sophisticated cyber espionage tool developed by Turla, a state-sponsored group believed to be a unit within Russia's Federal Security Service (FSB). Turla has been targeting various entities, including NATO-affiliated countries, journalists, and more recently, Middle Eastern nations. Snake infiltrated computer systems and exfiltrated stolen documents through a covert network of unwittingly compromised computers globally. The operation, codenamed MEDUSA, utilized a powerful tool called PERSEUS developed by the Federal Bureau of Investigation (FBI).

Snake is a covert long-term intelligence collection tool that creates a peer-to-peer (P2P) network of compromised systems globally, and its modular architecture allows for efficient injection or modification of components. However, the US government was successful in issuing self-destruct commands to Snake, causing it to disable itself without affecting the host computer or legitimate applications. While this is a significant victory against cyber threats, it is essential for individuals and organizations to maintain vigilance against evolving cyber threats.

Implementing robust cybersecurity measures, such as strong passwords, regular software updates, and user education, can help safeguard against sophisticated attacks. Armoryze's **Managed Detection and Response** service can help organizations proactively detect and respond to advanced threats before they cause damage. It is vital to stay informed and stay secure in the ever-changing landscape of cybersecurity.